UNIT 11 : POLYNOMIAL RINGS

UNIT STRUCTURE

11.1 Learning Objectives

11.2 Introduction

11.3 Polynomial Rings : Definition and Examples

11.4 Properties of Polynomial Rings

11.5 Irreducible Polynanials : Definition and Example

11.6 Properties of Irreducible Polynomials

11.7 Irreducibility Tests

11.8 Structure of Finite Fields

11.9 Properties of Finite Fields

11.10 Let Us Sum Up

11.11 Further Readings

11.12 Answers To Check Your Progress

11.13 Model Questions

11.1 LEARNING OBJECTIVES

After going through this unit, you will able to-

- learn about the polynomial rings over commutative ring and integral domain
- learn about the irreducible polynomials and irreducibility tests
- learn about structure of finite fields.

11.2 INTRODUCTION

One of the mathematical concepts that learners are most familiar with and most comfortable with is that of a polynomial. In school every learner who opts for Mathematics comes accross the concept of polynomials, their addition, multiplication and factorization.

Also a learner taught to find solutions of polynomial equations. Later, at the beginning of college educations, the polynomial functions, their limits and continuity are also taught. In this unit, we want to discuss the polynomials,

but not essentially from any point of view as mentioned above, instead we shall treat polynomials as numbers of some ring and study the algebraic properties of that ring

In this unit, we also study about structure of finite fields. Finite fields were first introduced by Galois in 1830 in his proof of the unsolvability of the general quintic equation. When Cayley invented matrices a few decades later, it was natural to investigate groups of matrices over finite fields. To this day, matrix groups over finite fields are among the most important classes of groups. In the past 50 years, there have been important applications of finite fields in computer science, coding theory, information theory and cryptography.

11.3 POLYNOMIAL RINGS : DEFINITION AND EXAMPLES

Definition (Ring of polynomial over R) Let R be a commutative ring. The set

$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 | a_i \in R$ and n is a nonnegative integer$\}$ is called the ring of polynomials over R in the indeterminate x.

Two elements

$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$

and $b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$

of R[x] are considered equal if and only if $a_i = b_i$ for all nonnegative integees i. (Define $a_i = 0$ when i>n and $b_i = 0$ when i>m)

To make R[x] into a ring, we define addition and multiplication in the usual way.

Definition 11.3.2 (Addition and multiplication in R[x]. Let R be a commutative ring and let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$

and $b_m x^m + a_{m-1}x^{m-1} + \ldots + b_1 x + b_0$ belong to R[x]. Then

$f(x) + g(x) = (a_s + b_s)x^s + (a_{s-1} + b_{s-1})x^{s-1} + \ldots + (a_1 + b_1)x + (a_0 + b_x)$

Where $s = \max\{m, n\}$, $a_i = 0$ for $i > n$ and $b_i = 0$ for $i > m$. Also

$f(x)g(x) = C_{m+1}x^{m+n} + C_{m+n-1}x^{m+n-1} + \ldots + C_1 x + C_0$,

When $C_k = a_k b_0 + a_{k-1}b_1 + \ldots + a_1 b_{k-1} + a_0 b_k$

for k = 0, 1, 2, . . ., m+n

i.e. $C_0 = a_0b_0$

$C_1 = a_1b_0+a_0b_1$

$C_2 = a_2b_0+a_1b_1+a_0b_2$

$C_3 = a_3b_0+a_2b_1+a_1b_2+a_0b_3$

.....

.....

$C_{m+n} = a_{m+n}b_0+a_{m+n-1}+a_{m+n-2}b_2+ \ . \ . \ . \ + a_0b_{m+n}$

It is time to introduce some terminology for polynomials.

If $f(x) = a_0x^n+a_{n-1}x^{n-1}+ \ . \ . \ . \ +a_1x+a_0$

Where $a_n \neq 0$, we say that f(x) has degree n; the term a_n is called the leading coefficient of f(x), and if the leading coefficient is the multiplicative identity element of R, we say that f(x) is a monic polynomial. The polynomial f(x)=0 has no degree. Polynomials of the form $f(x) = a_0$ are called constant. We write deg f(x) = n to indicate that f(x) has degree n.

Example 1. Consider $f(x) = 2x^3+x^2+2x+2$

and $g(x) = 2x^2+2x+1$ in $Z_3[x]$.

Then, in our preceding notation.

$a_5=0, a_4=0, a_3=2, a_2=1, a_1=2, a_0=2$

$b_5=0, b_4=0, b_3=0, b_2= 1, b_1=2, b_0=2$

Now using the definitions and remembering that addition and multiplication of the coefficients are done modulo 3, we have

$f(x)+g(x) = (a_3+b_3)x^3+(a_2+b_2)x^2+(a_1+b_1)x+(a_0+b_0)$

$= (2+0)x^3+(1+2)x^2+(2+2)x+(2+1)$

$= 2x^3+0.x^2+1.x + 0$

$= 2x^3 + x$

and $f(x).g(x) = C_5x^5+C_4x^4+C_3x^4+3_3x^3+C_2x^2+C_1x+C_0$

When $C_5 = a_5b_0+a_4b_1+a_3b_2+a_2b_3+a_1b_4+a_0b_5$

$= 0.1 + 0.2 +2.2 + 1.0 + 2.0 + 2.0$

$= 1$

$C_4 = a_4b_0+a_3b_1+a_2b_2+a_1b_2+a_1b_3+a_0b_4$

$= 0.1 + 2.2 +1.2 + 1.0 + 2.0$

$= 0$

$C_3 = a_3b_0+a_2b_1+a_1b_2+a_0b_3$

$= 2.1+2.2 + 1. + 2.0 + 2.0$

$= 2$

$C_2 = a_2b_0+a_1b_1+a_0b_2$

$= 1.1 + 2.2 + 2.2$

$= 0$

$C_1 = a_1b_0+a_0b_1$

$= 2.1 + 2.2$

$= 0$

$C_0 = a.b_0$

$= 2.1$

$= 2$

$\therefore$ $f(x).g(x) = 1.x^5 + 0.x^4 + 2x^3 + 0.x^2 + 0.x + 2$

$= x^5+2x^3+2$

Example 2. Consider $f(x) = 1+2x+2x^2–4x^3$

and $g(x) = 3 – 4x +2x^2$ in $Z(x)$.

Then $f(x)+g(x) = (1+3) + (2–4)x +(3+2)x^2 +(–4+0)x^3$

$= 4 – 2x + 5x^2 – 4x^3$

Here $a_5= 0, a_4=0, a_3=– 4, a_2=3, a_1=2, a_0=1$

$b_5= 0, b_4=0, b_3=0, b_2= 2, b_1=–4, b_0=3$

Now $f(x)g(x) = C_5x^5 + C_4x^4+C_3x^3+C_2x^2 + C_1x + C_0$

Where $C_5 = a_5b_0+a_4b_1+a_3b_2+a_2b_3+a_1b_4+a_0b_5$

$= 0.3 + 0.(– 4) +(– 4).2 + 3.0 + 2.0 + 1.0$

$= – 8$

$C_4 = a_4b_0+a_3b_1+a_2b_2+a_1b_2+a_1b_3+a_0b_4$

$= 0.3 + (–4). (–4) + 3.2 + 2.0 + 1.0$

$= 22$

$C_3 = a_3b_0+a_2b_1+a_1b_2+a_0b_3$

$= –4.3+3.(–4) + 2.2 + 1.0$

$= – 20$

$C_2 = a_2b_0+a_1b_1+a_0b_2$

$= 3.3 + 2.(–4) + 1.2$

$= 2$

$C_1 = a_1b_0+a_0b_1$

$= 2.3 + 1.(-4)$

$= 2$

$C_0 = a_0b_0$

$= 1.3$

$= 3$

$\therefore$ $f(x).g(x) = (-8)x^5 + 22x^4 + (-20)x^3 + 3.x^2 + 2.x + 3$

$= -8x^5+2x^4-20x^3+3x^2+2x+3$

Heme deg $\{f(x) + g(x) = 2$ and deg $\{f(x)g(x)\} = 5$

Remark : Let R[x] be the set of all polynomial over R. Then R[x] is a non empty set and addition and multiplication as defined above on the members of R[x], clearly these are binary compositions. It is easy to see that R[x] forms a ring under these operations. Zero of the ring will be the zero polynomial.

$0(x) = 0 + 0x + 0x^2 + \ldots$

Additive inverse of $f(x) = a_0 + a_1x + \ldots + a_mx^m$ will be the polynomial $-f(x) = -a_0 - a_1x - \ldots - a_mx^m$.

In fact, if R has unity 1, then the polynomial $e(x) = 1+0.x+0.x^2 + \ldots$ will be unity of R[x].



CHECK YOUR PROGRESS

Q 1: Let $f(x) = 1+2x+3x^2 \in Z_6[x]$ and $g(x) = 2+4x+2x^2 \in Z_6[x]$. Find f(x)+g(x), f(x).g(x), deg {f(x)+g(x)}, deg {f(x).g(x)}.

Q 2: Find the sum and product of

$f(x) = 2+3x+4x^2+2x^3$

$g(x) = 4+2x+3x^4$, where $f(x), g(x) \in Z_5[x]$

Also find deg {f(x)+g(x)} and deg {f(x).g(x)}

Q 3: Let R be any ring. Then show that the set R[x] of all polynomials in x over R is also a ring.

11.4 PROPERTIES OF POLYNOMIAL RINGS

Throrem 11.4.1 Let R[x] be the polynomial ring over a ring R. Then

(i) R is commutative if and only if R[x] is commutative.

(ii) R has unity of and only if R[x] has unity.

Proof : Let R[x] be a commutative polynomial ring. We have to prove R is commutative.

Since R[x] is commutative polynomial ring, therefore any subring of R[x] is commutative.

Define $f : R \to R[x]$ by

$f(a) = a+0.x+0x^2 + \ldots$

It is easy to see that f will be 1–1 homomorphism.

Indeed,

$f(a+b) = (a+b)+0.x+0.x^2 + \ldots$

$= (a+0.x+0.x^2+ \ldots) + (b+0.x+0.x^2+ \ldots)$

$= f(a) + f(b)$

and $f(ab) = ab+0.x+0.x^2 + \ldots$

$= (a+0.x+0.x^2 + \ldots) (b+0.x+0.x^2 + \ldots)$

$= f(a)\, f(b)$

Hence R can be imbedded into the ring R[x]. In other words, R is isomorphic to a subring of R[x]. As any saving of R[x] is commutative and R is isomorphic to a subring of R[x], R will be commutative.

Conversely, let R be a commutative ring. We have to prove R[x] is commutative. Let

$f(x) = a_0+a_1x+a_2x^2 + \ldots + a_mx^m$

$g(x) = b_0+b_1x+b_2x^2 + \ldots + b_nx^n$

be two members of R[x]. Then by definition of polynomial multiplication,

$f(x).g(x) = c_0+c_1x+c_2x^2+ \ldots + c_tx^t$ where $t \leq m+n$ and $c_k = \sum_{i+j=k} a_ib_j$

Also $g(x).f(x) = d_0+d_1x+d_2x^2 + \ldots + d_tx^t$ where $t \leq m+n$ and $d_k = \sum_{j+i=k} b_ja_i$

Now $c_k = \sum_{i+j=k} a_ib_j$

$= a_0b_k + a_1b_{k-1}+a_2b_{k-2}+ \ldots + a_ib_j + \ldots + a_kb_0$

$= b_ka_0 + b_{k-1}a_1+b_{k-2}a_2+ \ldots + b_0a_k$ [$\because$ R is commutative]

$= b_0a_k + b_1a_{k-1}+ \ldots + b_{k-2}a_2+b_{k-1}a_1+b_ka_0$

$$= \sum_{j+i=k} b_j a_i$$

$$= d_k$$

$\therefore\ c_k = d_k\ \forall\ k$

Thus $f(x).gx) = g(x).f(x)$ for all $f(x), g(x) \in R[x]$.

$\Rightarrow R[x]$ is a commutative polynomial ring.

(ii) Let R be a ring with unity 1. We have to prove R[x] is a polynomial ring with unity.

Consider $e(x) = 1+0.x+0.x^2 + \ldots$ Clearly $e(x) \in R[x]$

and for any $f(x) = a_0+a_1x+a_2x^2 + \ldots + a_nx^n \in R[x]$,

$f(x).e(x) = (a_0+a_1x+a_2x^2+ \ldots +a_nx^n)\ (1+0.x+0.x^2 + \ldots)$

$= a_0+a_1x+a_2x^2+ \ldots +a_nx^n$

$= f(x)$

Similarly, $e(x).f(x) = f(x)$

Thus $e(x) = 1+0.x+0.x^2 + \ldots$ is the unity in R[x].

Conversely, let R[x] have unity. We have to prove R is commutative.

Define a map $\theta : R[x] \to R$

by $\theta(f(x)) = \theta(a_0+a_1x_+a_2x^2+ \ldots +a_mx^m)$

$= a_0$

Let $f(x) = a_0+a_1x+a_2x^2+ \ldots + a_mx^m \in R[x]$ and

$g(x) = b_0+b_1x+b_2x^2+ \ldots + b_nx^n \in R[x]$, Then

$\theta(f(x)) = a_0, \theta\ (g(x)) = b_0$ and

$f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+ \ldots +(a_t+b_t)x^t$

Where $a_t = 0$ when $t > m$

$b_t = 0$ when $t > n$

$f(x).g(x) = c_0+c_1x+c_2x^2 + \ldots + c_kx^k$ where

$$c_k = \sum_{i+j=k} a_i b_j$$

Now $\theta(f(x) + g(x)) = a_0+b_0$

$= \theta(f(x)+\ \theta\{g(x))$

and $\theta\{f(x).g(x)\} = c_0$

$= a_0b_0$

$= \theta\{f(x)\}.\theta\{g(x)\}$

Hence θ is a ring homomorphism.

Also for any $a \in R$, $\exists$ a polynomial $f_a(x) = a+0.x+0x^2 + \ldots \in R[x]$ such that

$\theta(f_a(x)) = a$

Thus θ is onto and hence R is a homomorphic image of R[x]. As homomorphic image of a ring with unity is a ring with unity. In fact,

$\theta(e(x)) = \theta(1+0x+0x^2+\ldots)$

$= 1$

will be the unity of R.

Theorem 11.4.2. Let R[x] be the polynomial ring of a ring R and suppose

$f(x) = a_0+a_1x+a_2x^2+\ldots+a_mx^m \in R[x]$

and $g(x) = b_0+b_1x+b_2x^2+\ldots+b_nx^n \in R[x]$

are two non zero polynomials of degree m and n respectively. Then

(i) If $f(x)+g(x) \neq 0$, then deg $(f(x)+g(x)) \leq \max\{m, n\}$

(ii) If $f(x).g(x) \neq 0$, then deg $(f(x).g(x)) \leq m+n$

(iii) If R is an integral domain, then

deg(f(x).g(x)) = m+n

(iv) R is integral domain if and only if R[x] is an integral domain.

(v) If R is a field, then R[x] may not be a field.

Proof : Let R[x] be the polynomial ring over the ring R and suppose

$f(x) = a_0+a_1x+a_2x^2+\ldots+a_mx^m$

$g(x) = b_0+b_1x+b_2x^2+\ldots+b_nx^n$

be two nonzero polynomial in R[x]

(i) Let $f(x) + g(x) \neq 0$ and

$f(x)+g(x) = c_0+c_1x+c_2x^2+\ldots+c_tx^t$

Where $c_i = a_i+b_i$ and $a_t = 0$ when $t>m$, $b_t = 0$ when $t>n$.

Let $s = \max\{m, n\}$. Then

$c_t = a_t+b_t = 0$ when $t>s$.

$c_s = a_s+b_s$

$$= \begin{cases} a_m, & \text{if } s = m > n \\ b_n, & \text{if } s = n > m \\ a_m + b_m, & \text{if } s = m = n \\ 0, & \text{if } a_m + b_m \neq 0 \end{cases}$$

Thus deg $\{f(x)+g(x)\} = \begin{cases} m, \text{ if } m > n \\ n, \text{ if } n > m \\ m, \text{if } m = n \quad a_m + b_m \neq 0 \end{cases}$

and deg $\{f(x)+g(x)\} < m$ if $m = n$, $a_m+b_m = 0$

Hence deg $\{f(x)+g(x)\} = \begin{cases} \max\{m, n\} \text{ if } m \neq n \\ m, \text{ if } m = n, \ a_m + b_m \neq 0 \\ < m \text{ if } m = n, \ a_m + b_m = 0 \end{cases}$

$\Rightarrow$ deg $\{f(x)+g(x) \leq \max\{ m, n)$

(ii) Let $f(x).g(x) \neq 0$ and

$f(x).g(x) = c_0+c_1x+c_2x^2+ \ldots +c_kx^k+ \ldots$

Where $c_k = \sum_{i+j=k} a_ib_j$

Hence $c_{m+n} = a_0 b_{m+n}+a_1 b_{m+n-1}+ \ldots + a_mb_n+a_{m+1}b_{n-1}+ \ldots + a_{m+n}b_0$

$= a_mb_n$

as all other terms would be zero since $a_{m+i} = 0$, $b_{n+j} = 0$ for all $i, j > 0$.

Again $C_{m+n+t} = 0$ for all $t > 0$ and

thus deg $(f(x).g(x)) \leq m+n$ (a_mb_n can be zero even if $a_m \neq 0$, $b_n \neq 0$).

(iii) If R is an integral domain, then as $a_m \neq 0$, $b_n \neq 0$, therefore $a_mb_n \neq 0$ and hence $c_{m+n} = a_mb_n \neq 0$ showing that deg $(f(x).g(x)) = m+n$.

(iv) If R[x] is an integral domain, then since R is isomorphic to a subring of R[x], R will also be an integral domain.

Conversely, suppose R is an integral domain. We have to prove R[x] is also an integral domain.

Let f(x), g(x) be any two non-zero members of R[x] such that

$f(x).g(x) = 0$

Where $f(x) = a_0+a_1x+a_2x^2 + \ldots + a_mx^m$

$g(x) = b_0+b_1x+b_2x^2+ \ldots +b_nx^n$

If f(x) and g(x) are both constant polynomials, then

$a_0 \neq 0$, $b_0 \neq 0$

and so $c_0 = a_0b_0 \neq 0$ imples $f(x)g(x) \neq 0$

Which is a contradiction.

Again, if at least one of f(x), g(x) is non constant polynomial, its degree is ≥ 1 and

$\deg(f(x)) + \deg(g(x)) \geq 1$

R being an integral domain,

$\deg(f(x).g(x)) = \deg(f(x)) + \deg(g(x)) \geq 1$

$\Rightarrow f(x).g(x) \neq 0$

Which is also a contradiction. Hence

$f(x)\, g(x) = 0$

$\Rightarrow f(x) = 0$ or $g(x) = 0$

$\Rightarrow$ R[x] is an integral domain.

(v) Let F be a field. Then F is commutative with unity. So F[x] will be commutative ring with unity. In fact, F being an integral domain., F[x] will also be an integral domain. We show, not all nonzero elements of F[x] have multiplicative inverse. Consider a non-zero polynomial

$f(x) = 0+1.x+0x^2+0.x^3+ \ldots$

suppose $g(x) = b_0+b_1+b_2x^2 + \ldots$ is its multiplicative inverse. Then

$f(x)g(x) = c_0+c_1x+c_2x^2 + \ldots$

$= e(x)$

$= 1+0.x+0.x^2 + \ldots$

Which implies $c_0=1$, $c_i=0$ for all $i> 0$

But $c_0 = a_0b_0 = 0.b_0 = 0 \neq 1$

Hence no g(x) can be multiplicative inverse of f(x) = x and which showing that F[x] is not a field.

Theorem 11.4.3. If A be an ideal of a ring R, then A[x] is an ideal of the polynomial ring R[x].

Proof : $A[x] = \{f(x) : f(x) = a+a_1x+a_2x^2+ \ldots +a_nx^n, a_0, a_1, a_2, \ldots, a_n \in A\}$.

As A is an ideal of R and $0 \in A$,

$0 \in A[x]$

$\Rightarrow A[x] \neq \phi$

Let $f(x), g(x) \in A[x]$, where

$f(x) = a_0+a_1x+a_2x^2+ \ldots + a_mx^m; a_0, a_1, a_2, \ldots a_m \in A$

and $g(x) = b_0+b_1x+b_2x^2+ \ldots + b_mx^n; b_0, b_1, b_2, \ldots b_n \in A$

Then $f(x)–g(x) = (a_0–b_0)+(a_1–b_1)x+(a_2–b_2)x^2+ \ldots +c_tx^t$

Where $t \leq \max\{m, n\}$.

Since $a_i–b_i \in A$ for all i, so

$f(x) - g(x) \in A[x]$

Let $h(x) = r_0+r_1x+r_2x^2+ \ldots + r_px^p \in R[x]$. Then

$h(x)\, f(x) = d_0+d_1x_{+d}2_x^{\,2}+ \ldots .+d_lx^l$

Where $d_k = \sum_{i+j=k} r_i\, a_j$; $0 \le k \le l$ and $l \le p+m$

$\in A$ [$\because r_1 \in R, a_j \in A \quad \Rightarrow r_ia_j \in A$]

Hence $h(x)\, f(x) \in A[x]$

Similarly $f(x)\, h(x) \in A[x]$

Thus A[x] is an ideal of R[x]

Theorem 11.4.4. If R is a ring, then the set of all polynomial in R[x] which have constant term zero form a subring of R[x].

Proof : Let $S[x] = \{f(x) = a_1x+a_2x^2 + \ldots + a_mx^m ; a_1, a_2, \ldots a_m \in R\}$

Since $0 = 0.x + 0.x^2 + \ldots \in S[x]$, so $S[x] \neq \phi$.

Let $f(x), g(x) \in S[x]$, where

$f(x) = a_0+a_1x+a_2x^2+ \ldots + a_mx^m ; a_0, a_1, a_2, \ldots , a_m \in R, a_0 = 0$

$g(x) = b_0+b_1x+b_2x^2+ \ldots + b_nx^m; b_0, b_1, b_2, \ldots , b_n \in R, b_0 = 0$

Then $f(x) - g(x) = c_0+c_1x+c_2x^2+ \ldots + c_tx^t$

Where $c_i = a_i-b_i \ \forall$ i = 0, 1, 2, 3, . . ., t and $t \le \max\{m, n\}$

$\in R$

and $c_0 = a_0-b_0 = 0$ [$\because a_1, b_i \in R \quad \Rightarrow a_i-b_i \in R$]

Thus $f(x) - g(x) \in S[x]$

Next $f(x)\, g(x) = d_0+d_1x+d_2x^2 + \ldots + d_px^p$

Where $d_k = \sum_{i+j=k} a_ib_j \in R$ for all k = 0, 1, 2, . . ., p and $p \le m+n$.

Now $d_0 = a_0b_0 = 0.0 = 0$ and $d_1, d_2, \ldots d_p \in R$

Thus $f(x).g(x) \in S[x]$

Hence S[x] is a subring of R[x].

The Division Algorithm and Consequences :

One of the properties of integers that we have used repeatedly is the division algorithm : If a and b are integers and $b \neq 0$, then there exist unique integers q and r such that $a = bq+r$ where $0 \le r<|b|$. The next theorem is the analogous statement for polynomials.

Theorem 11.4.5. (Division Algorithm in R[x]) Let R be a commutative ring unity and g(x), a nonzero polynomial in R[x] of degree n with leading coefficient b_n unit in R. Then for any $f(x) \in R[x]$ there exist unique polynomials q(x), r(x) in R[x] such that

$f(x) = g(x)\, q(x) + r(x)$

where r(x) = 0 or deg r(x) <deg g(x).

Proof : First let f(x) = 0. Then we can write 0 = f(x) = g(x).0+0

Here q(x) = 0 and r(x) = 0

Thus the result holds if f(x) = 0

Next, let $f(x) \neq 0$ and deg f(x) < deg g(x). Then we can write f(x) = g(x).0 + f(x). Here q(x) = 0 and r(x) = f(x).

So the result holds if $f(x) \neq 0$ and deg f(x) <deg g(x).

Next, let $f(x) \neq 0$ and deg $f(x) \geq$ deg g(x).

If deg f(x) = 0, then deg g(x) = 0 and f(x) and g(x) are both constant polynomials.

Let $f(x) = a_0$, $g(x) = b_o$. By the given condition,

b_0 is unit in R

$\Rightarrow b_0^{-1}$ exists in R such that $b_0^{-1}b_0 = 1 = b_0b_0^{-1}$

Now $a_0 = a_0 + 0$

$= 1.a_0.1+0$

$= (b_0b_0^{-1})\, a_0 + 0$

$= b_0(b_0^{-1}a_0) + 0$

i.e. $f(x) = g(x)\, q(x)+r(x)$, where $q(x) = b_0^{-1}a_0$

and r(x) = 0

Thus the result holds if f(x) is a polynomial of degree zero.

We assume the result holds for every polynomial f(x) of degree less than m.

We consider a polynomial f(x) of degree m,

i.e. Let $f(x) = a_0+a_1x+a_2x^2+. \ . \ .+a_mx^m$ (1)

$g(x) = b_0+b_1x+b_2x^2+. \ . \ .+b_nx^n$ (2)

Where b_n is a unit in R and $m \geq n$.

Multiplying g(x) by $a_mb_n^{-1}\, x^{m-n}$, get

$a_mb_n^{-1}\, x^{m-n}\, g(x) = b_0(a_mb_n^{-1})x^{m-n}+b_1(a_mb_n^{-1})x^{m-n+1}+ \ . \ . \ .+ \ a_mx^m$ (3)

From (1) and (3), $f(x) - a_m b_n^{-1} x^{m-n} g(x)$ is either zero or a polynomial of degree less than m.

If $f(x) - a_m b_n^{-1} x^{m-n} g(x) = 0$, then

$$f(x) = a_m b_n^{-1} x^{m-n} g(x)$$
$$= g(x).a_m b_n^{-1} x^{m-n} + 0$$
$$= g(x).q(x) + r(x)$$

Where $q(x) = a_m b_n^{-1} x^{m-n}$ and $r(x) = 0$

If $f(x) - a_m b_n^{-1} x^{m-n} g(x)$ is a polynomial of degree less than m, then by induction hypothesis there exists polynomial $q_1(x)$ and $r_1(x)$ such that

$$f(x) - a_m b_n^{-1} x^{m-n} g(x) = g(x)\, q_1(x) + r_1(x)$$

Where either $r_1(x) = 0$ or $\deg r_1(x) < \deg g(x)$.

This implies that

$$f(x) = g(x).\, [a_m b_n^{-1} x^{m-n} + q_1(x)] + r_1(x)$$
$$= g(x).q(x) + r(x) \quad \text{(say)}$$

Where $q(x) = a_m b_n^{-1} x^{m-n} + q_1(x)$ and $r(x) = r_1(x)$.

Hence the result holds for a polynomial f(x) of degree m.

To prove uniqueness, suppose that $f(x) = g(x)q(x) + r(x)$ and $f(x) = g(x)\, q'(x) + r'(x)$, where $r(x) = 0$ or $\deg (r(x)) < \deg g(x)$ and $r'(x) = 0$ or $\deg r'(x) < \deg g'(x)$.

Now $g(x)q(x)+r(x) = g(x)q'(x)+r'(x)$

$$\Rightarrow g(x)\, [g(x)-q'(x)] = r'(x) - r(x) \qquad (4)$$

If $q(x) - q'(x) \neq 0$, then

$$\deg[\{q(x) - q'(x)\}\, g(x)] = \deg[q(x)-q'(x)]+\deg g(x) \geq \deg g(x)$$

$$\Rightarrow \deg[r'(x) - r(x)] \geq \deg g(x)$$

Which is a contradiction to the facts $\deg r(x) < \deg g(x)$ and $\deg r'(x) < \deg g(x)$.

Hence $q(x) - q'(x) = 0 \Rightarrow q(x) = q'(x)$

From (4), $r'(x) - r(x) = 0$

$$\Rightarrow r'(x) = r(x)$$

The polynomials q(x) and r(x) in the division algorithm are called the quotient and remainder in the division of f(x) by g(x).

Example : To find the quotient and remainder upon dividing $f(x) = 3x^4+x^3+2x^2+1$ by $g(x) = x^2+4x+2$, where f(x) and g(x) belong to $Z_5[x]$. We

may proceed by long division, provided we keep in mind that addition and multiplication are done modulo 5. Thus

$$
\begin{array}{r}
3x^2+4x \\
x^2+4x+2\overline{)\,3x^4+x^3+2x^2\quad+1} \\
\underline{3x^4+2x^3+x^2} \\
4x^3+x^2\quad+1 \\
\underline{4x^3+x^2+3x} \\
3x+1
\end{array}
$$

So $3x^2+4x$ is the quotient and $3x+1$ is the remainder. Therefore

$3x^4+x^3+2x^2+1 = (x^2+4x+2)(3x^2+4x)+(3x+1)$

Corollary 11.4.6. Let F be a field and let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exists unique polynomials q(x) and r(x) in F[x] such that f(x) = g(x)q(x)+r(x) where

wither r(x) = 0 or deg r(x) < deg g(x).

Factor, zero and zero of multiplicity k($k \geq 1$) :

Definition: Let D be an integral domain. If f(x) and $g(x) \in D[x]$, we say that g(x) divides f(x) in D[x] and write g(x)|f(x) if there exists an $h(x) \in D[x]$ such that f(x) = g(x).h(x). In this case, we call g(x) a factor of f(x). An element a is a zero (or a root) of a polynomial f(x) if f(a) = 0. When F is a field, $a \in F$ and $f(x) \in F[x]$, we say that a is a zero of multiplicity k($k \geq 1$) if $(x-a)^k$ is a factor of f(x) but $(x-a)^{k+1}$ is not a factor of f(x).

Corollary 11.4.8 (Remainder Theorem) : Let F be a field, $a \in F$ and $f(x) \in F[x]$. Then f(a) is the remainder in the division of f(x) by x–a.

Corollary 11.4.9. (Factor Theorem) : Let F be a field, $a \in F$ and $f(x) \in F[x]$. Then a is a zero of f(x) if and only if x–a is a factor of f(x).



CHECK YOUR PROGRESS

Q 4: Let R be a commutative ring with unity. Let A be an ideal of R. Show that $R[x]/A[x] \cong R/A\,[x]$.

Q 5: For any commutative ring R with unity, show that $R[x]/\langle x \rangle \cong R$.

Q 6: Let R be a commutative ring with unity and $\langle x \rangle$ be a prime idea of R[x]. Show that R must be an integral domain.

11.5 IRREDUCIBLE POLYNANIALS : DEFINITION AND EXAMPLE

Definition: Irreducible Polynomial, Reducible Polynomial

Let D be an integral domain. A polynomial f(x) from D[x], i.e., neither the zero polynomial nor a unit in D[x] is said to be irreducible over D if, whenever f(x) is expressed as a product f(x) = g(x) h(x), with g(x) and h(x) from D[x], then g(x) or h(x) is a unit in D[x]. In other words. A polynomial $f(x) \in D[x]$ of positive degree (i.e., of $\deg \geq 1$) is said to be an irreducible polynomial over D if it cannot be expressed as product of two polynomials of positive degree, i.e. if whenever f(x) = g(x) h(x), then deg g(x) = 0 or deg h(x) = 0.

Example 1. $x^2+1 \in z[x]$ is irreducible over Z because it can not be expressed as product of two polynomials of positive degree over Z. Whereas it is reducible over C as $x^2+1 = (x+i)(x-i)$

Example 2. x^2-2 is irreducible over Z because it can not be expressed as product of two polynomials of positive degree over Z. Whereas it is reducible over R as $x^2-2 = x^2 - \left(\sqrt{2}\right)^2$

$$= \left(x+\sqrt{2}\right)\left(x-\sqrt{2}\right)$$

The polynomial x^2-2 is irreducible over Q because it cannot be expressed as product of two polynomials of positive degree over Q.

Example 3. The polynomial $f(x) = 2x^2 + 4$ is irreducible but reducible over Z, since $2x^2+4 = 2(x^2+2)$ and neither 2 nor x^2+2 is a unit in Z [x].

The polynomial $f(x) = 2x^2+4$ is irreducible but reducible over Z, since $2x^2+4 = 2(x^2+2)$ and neither 2 nor x^2+2 is a unit in Z[x].

The polynomial $f(x)=2x^2+4$ is irreducible over R but reducible over C.

Remarks : (a) Any polynomial of degree 1 is irreducible over a field F.

(b) If $f(x) \in F[x]$ is any polynomial of degree 2 or 3 and f(a) = 0 for some $a \in F$, then f(x) is reducible over F.

f(x) is reducible

$\Rightarrow$ f(x) = g(x) h(x) where deg g(x), deg h(x) ≥ 1

Now deg f(x) = deg g(x) + deg h(x)

$\Rightarrow$ deg g(x) + deg h(x) = 2 or 3

$\Rightarrow$ at least one of g(x) and h(x) has degree 1.

Let deg g(x) = 1 and g(x) = ax+b. Then clearly $-a^{-1}b$ is a zero of g(x) and therefore a zero of f(x) as well.

Example 4. The polynomial x^2+1 is irreducible over Z_3 because neither 0, 1 nor 2 is a zero of x^2+1 over Z_3. Where as x^2+1 is reducible over Z_5 because 2 is zero of x^2+1 over Z_5.

Note : Polynomials of degree larger than 3 may be reducible over a field even though they donot have zeros in the field. For example, in Q[x], the polynomial $x^4+2x^2+1 = (x^2+1)^2$, but has no zeros in Q.



CHECK YOUR PROGRESS

Q 7: Show that the following polynomials are irreducible over Q,

(i) $8x^3 - 6x - 1$

(ii) $x^4 + x^3 + x^2 + x + 1$

Q 8: Give an example of a polynomial which is irreducible over R and reducible over C.

Q 9: Show that x^2+1 and x^2+x+4 are irreducible over Z_{11}.

Definition: An element p in a commutative ring with unity is called irreducible if

(i) $p \neq 0$ and p is not a unit.

(ii) Whenever p = ab, then one of a and b must be unit; in over words p has no proper factors.

Example 1. In z every prime number is an irreducible element.

Example 2. In $Z\left[\sqrt{-5}\right] = \left\{a+b\sqrt{-5} : a, b \in Z\right\}$, 1 and –1 are the only units. We claim that 3 is irreducible element in $Z\left[\sqrt{-5}\right]$. If not, then let

$3 = \left(a+b\sqrt{-5}\right)\left(c+d\sqrt{-5}\right)$ for some a, b, c, d $\in Z$

Where both $a+b\sqrt{-5}$ and $c+d\sqrt{-5}$ are non-units.

Also $3 = \left(a-b\sqrt{-5}\right)\left(c-d\sqrt{-5}\right)$

Thus $9 = \left(a^2+5b^2\right)\left(c^2+5d^2\right)$

$\Rightarrow$ either $a^2+5b^2 = 1$ and $c^2+5d^2 = 9$

or $a^2+5b^2 = 3$ and $c^2+5d^2 = 3$

or $a^2+5b^2 = 9$ and $c^2+5d^2 = 1$

Since 5 > 1, the only integral solutions of $a^2+5b^2 = 1$ are $a=\pm 1$, $b = 0$. Also $a^2+5b^2 = 3$ has no integral solution. In case $a^2+5b^2 = 9$, $c^2+5d^2 = 1$, we get $c = \pm 1$, $d = 0$. Thus

$$3 = \left(a+b\sqrt{-5}\right)\left(c+d\sqrt{-5}\right)$$

$\Rightarrow a+b\sqrt{-5} = \pm 1$ or $c+d\sqrt{-5} = \pm 1$

Hence 3 is an irreducible element in $Z\left[\sqrt{-5}\right]$.

Example 3. In Z[i], the ring of Gaussian Integers, 1+i is an irreducible element. Suppose

$1+i = (a+ib)(c+id)$ where $a, b, c, d \in Z$

and then $1-i = (a-ib)(c-id)$

$\therefore\ 1^2+1^2 = (a^2+b^2)(c^2+d^2)$

$\Rightarrow (a^2+b^2)(c^2+d^2) = 2$

$\Rightarrow a^2+b^2 = 1, c^2+d^2 = 2$ or $a^2+b^2 = 2, c^2+d^2 = 1$

In case $a^2+b^2 = 1$, $(a+ib)(a-ib) = 1$

$\Rightarrow$ a+ib is unit.

In case $c^2+d^2 = 1$ $(c+id)(c-id) = 1$

$\Rightarrow$ c+id is unit.

Hence 1+i is irreducible.

Definition: (Primitive Polynomial) : Let $f(x) = a_0+a_1x+a_2x^2+ \ldots + a_mx^m$ be a polynomial in Z[x]. If gcd $(a_0, a_1, a_2, \ldots, a_m) = 1$, then f(x) is called a primitive polynomial. Also gcd $(a_0, a_1, a_2, \ldots, a_n)$ is called content of the polynomial f(x).

Example 1. $2+3x-5x^2$ is a primitive polynomial because gcd (2, 3, –5) = 1.

Example 2. $3+6x+12x^2$ is not a primitive polynomial because gcd (3, 6, 12) $= 3 \neq 1$.

11.6 PROPERTIES OF IRREDUCIBLE POLYNOMIALS

Theorem 11.6.1. Let $f(z) \in Z[x]$. If f(x) is reducible over Q, then it is reducible over Z.

Proof : Suppose $f(x) = g(x).\ h(x)$, where g(x) and $h(x) \in Q[x]$. Clearly, we may assume that f(x) is primitive because we can divide both f(x) and

g(x) by the content of f(x).

Let a be the least common multiple of the denominators of the coefficients of g(x) and b be the least common multiple of the denominators of the coefficients of h(x). Then ab f(x) = ag(x). bh(x) where ag(x) and bh(x) $\in$ z(x).

Let c_1 be the content of ag(x) and let c_2 be the content of bh(x). Then $ag(x) = c_1g_1(x)$

and $bh(x) = c_2h_1(x)$ where $g_1(x)$ and $h_1(x)$ are primitive and $abf(x) = c_1c_2g_1(x)h_1(x)$.

Since f(x) is primitive, the content of abf(x) is ab.

Also product of two primitive polynomials is primitive, it follows that the content of $c_1c_2g_1(x)h_1(x)$ is c_1c_2. Thus $ab = c_1c_2$ and $f(x) = g_1(x)h_1(x)$ is c_1c_2. Thus $ab = c_1c_2$ and $f(x) = g_1(x)h_1(x)$.

Where $g_1(x), h_1(x) \in Z[x]$ and deg $g_1(x)$ = deg g(x) and deg $h_1(x)$ = deg.h(x). Hence f(x) is reducible over Z.

Theorem 11.6.2. Every irreducible element in R[x] is an irreducible polynomial, R being an integral domain with unity.

Proof: Let $f(x) \in R[x]$ be an irreducible element. We have to prove f(x) is an irreducible polynomial. Then f(x) = g(x) h(x) for some $g(x), h(x) \in R[x]$ with deg $g(x) > 0$, deg $h(x) > 0$.

Since deg $g(x) > 0$, deg $h(x) > 0$, so g(x) and h(x) are not constant polynomials and

$g(x), h(x) \notin R$

$\Rightarrow$ g(x), h(x) cannot be units in R.

$\Rightarrow$ g(x), h(x) cannot be units in R[x].

$\Rightarrow$ f is not irreducible element.

Which is a contradiction. This contradiction implies that f(x) is an irreducible polynomial.

11.7 IRREDUCIBILITY TESTS

Theorem 11.7.1. Let p be a prime and suppose that $f(x) \in Z[x]$ with deg $f(x) \geq 1$. Let $\bar{f}(x)$ be the polynomial in $Z_p[x]$ obtained from f(x) by reducing all the coefficients of f(x) modulo p. If $\bar{f}(x)$ is irreducible over Z_p and deg $\bar{f}(x)$

= deg f(x), then f(x) is irreducible over Q.

Proof : Let $\bar{f}(x)$ be irreducible over Z_p and deg $\bar{f}(x)$ = deg f(x) where p is prime, $\bar{f}(x)$ be the polynomial in $Z_p[x]$ obtained from $f(x) \in Z[x]$ by reducing all coefficients of f(x) modulo p and deg $f(x) \geq 1$. We have to prove f(x) is irreducible over Q. If possible, let f(x) be reducible over Q. Then

f(x) = g(x) h(x) with g(x), $h(x) \in Z[x]$ and both g(x) and h(x) have degree less than that of f(x). Let $\bar{f}(x)$, $\bar{g}(x)$ and $\bar{h}(x)$ be the polynomials obtained from f(x), g(x) and h(x) by reducing all the coefficients modulo p. Then $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$

Also, we have deg $\bar{f}(x)$=deg f(x) and

deg $\bar{g}(x) \leq$ deg g(x) <deg $\bar{f}(x)$

deg $\bar{h}(x) \leq$ deg h(x) <deg $\bar{f}(x)$

Therefore $\bar{f}(x)$ is a reducible polynomial in $Z_p[x]$ and this contradicts our assumption that $\bar{f}(x)$ is irreducible over Z_p. Hence our assumption, f(x) is reducible over Q, is wrong. Thus f(x) is irreducible over Q.

Example 1. Let $f(x) = 21x^3 - 3x^2 + 2x + 9$. Then over Z_2, we have $\bar{f}(x) = x^3 + x^2 + 1$ and $\bar{f}(0) = 1$ and $\bar{f}(1) = 1$, we see that $\bar{f}(x)$ is irreducible over Z_2. Thus f(x) is irreducible over Q.

Example 2. Let $f(x) = 15x^4 - 10x^2 + 9x + 21$. Applying the Mod 2 to (x), we get $\bar{f}(x) = x^4 + x + 1$ and $\bar{f}(0) = 1$, $\bar{f}(1) = 1$, i.e. $\bar{f}(x)$ has no zeros in Z_2. Thus $\bar{f}(x)$ is irreducible over Z_2. This guarantees that f(x) is irreducible over Q.

Theorem 11.7.2 (Eisenstein's Criterion)

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in Z[x]$.

If there is a prime p such that $p \not| a_n$, $p | a_{n-1}, \ldots, p | a_0$ and $p^2 \not| a_0$ then f(x) is irreducible over Q.

Proof : Without loss of generality, we assume f(x) is a primitive polynomial (because if f(x) is not primitive, then $f(x) = df_1(x)$, where $f_1(x)$ is a primitive polynomial and d is a content of f(x). This means that if the theorem holds for $f_1(x)$ it holds for f(x)).

Let f(x) = p(x) q(x) where p(x), $q(x) \in [x]$ are non constant polynomials. Then by Theorem 11.6.1, there exist g(x), $h(x) \in Z[x]$ such that

f(x) = g(x) h(x)

Where $p(x) = \frac{a}{b}\, g(x)$, $q(x) = \frac{c}{d} h(x)$ for some $a, b, c, d \in Z$.

Here g(x) and h(x) are non constant polynomials over Z.

Let $g(x) = b_r x^r + b_{r-1} x^{r-1} + \ldots + b_1 x + b_0$

$h(x) = c_s x^s + c_s x^{s-1} + \ldots + c_1 x + c_0$

Where b's and c's are integers and $r > 0$, $s > 0$.

Since $f(x) = g(x) \cdot h(x)$, so

$a_0 = b_0 c_0$ and $a_n = b_r s$

Now $p | a_0 \Rightarrow p | b_0 c_0$

$\Rightarrow p | b_0$ or $p | c_0$

But $p^2 \nmid a_0$. so p cannot divide both b_0 and c_0.

Let $p | b_0$ and $p \nmid c_0$

Also, we have $p \nmid a_n \Rightarrow p \nmid b_r c_s$

$\Rightarrow p \nmid b_r$ and $p \nmid c_s$

Let k be the smallest suffix such that $p \nmid b_k$. Then $k > 0$ and $k \leq p < n$

and $p \nmid b_0, b_1, b_2, \ldots, b_{k-1}, pb_k$

Now $a_k = \sum_{i+j=k} b_i c_j$

$= b_0 c_k + b_1 c_{k-1} + b_2 c_{k-2} + \ldots + b_{k-1}$, so $p | b_k c_0$.

Since $p | a_k$ and $p | b_0, b_1, \ldots, b_{k-1}$, so $p | b_k c_0$.

But $p \nmid b_k$, so $p | b_k c_0 \quad p | c_0$, which is a contradiction. This contradiction implics that g(x) and h(x) are both cannot be non constant polynomials, so

p(x) and q(x) are both cannot be non constant polynomials

$\Rightarrow$ either deg p(x) = 0 or deg q(x) = 0

$\Rightarrow$ f(x) is irreducible over Q.

Remark : f(x) = g(x) h(x) if and only if f(x+a) = g(x+a) h(x+a)

$\Rightarrow$ f(x) is irreducible if and only if f(x+a) is irreducible.

Example 1. Consider the polynomial $f(x) = x^3 + bx + 12$ over Q. Here $a_0 = 12$, $a_1 = 6$, $a_2 = 0$, $a_3 = 1$.

Consider p = 3. Then

$3 | 12, 3 | 6, 3 | 0, 3 \nmid 1$ and $3^2 \nmid 12$

Thus by Eisenstein's Criterion, f(x) is irreducible over Q.

Corollary 11.7.3. For any prime p, the p^{th} cyclotomic polynomial

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

is irreducible over Q.

Proof : We have

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

Let $f(x) = \phi_p(x+1)$

$$= \frac{(x+1)^p - 1}{(x+1) - 1}$$

$$= \frac{(x^p + {}^pC_1 x^{p-1} + {}^pC_2 x^{p-2} + \ldots + {}^pC_{p-1} x + 1) - 1}{x}$$

$$= x^{p-1} + {}^pC_1 x^{p-2} + {}^pC_2 x^{p-3} + \ldots + {}^pC_{p-1}$$

Since p is a prime number, so

$p \mid {}^pC_{p-1}, {}^pC_{p-2}, \ldots, {}^pC_2, {}^pC_1$, p1 and $p^2 \nmid {}^pC_{p-1}$

By Eisenstein's Criterion,

$f(x) = \phi_p(x+1)$ is irreducible over Q.

$\Rightarrow \phi_p(x)$ is irreducible over Q.



CHECK YOUR PROGRESS

Q 10: Show that the following polynomials are irreducible over Q.

(i) $f(x) = 3x^5 + 15x^4 - 20x^3 + 10x + 20$

(ii) $f(x) = 3x^3 + 6x^2 + 2x + 6$

(iii) $f(x) = x^3 + 3x + 2$

11.8 STRUCTURE OF FINITE FIELDS

Recall that a field F has characteristic p if p is the smallest positive integer such that for every nonzero element a in F, we have pa = 0. If no such integer exists, then F has characteristic 0. If F is a finite field of characteristic p, then p is prime. Suppose that F is a finite field with n elements. Then na = 0 for all $a \in F$. Consequently, the characteristic of F must be p, where p is a prime dividing n, Also if F is a finite field of characteristic p, then the order of F is p^n for some $n \in N$.

Lemma 11.8.1. Let p be prime and D be an integral domain of characteristic p. Then

$a^{p^n}+b^{p^n}=(a+b)^{p^n}$ for all positive integer n.

Proof : We prove this lemma using mathematical induction on n. For n = 1

$$(a+b)^n = \sum_{k=0}^{p} {}^{p}C_k\, a^k b^{p-k}$$

If $o < k < p$, then ${}^{p}C_k = \frac{|\underline{p}}{|\underline{k}\,|\underline{p-k}}$ must be divisible by p, since p cannot divide $|\underline{k}\ |\underline{p-k}$. Note that D is an integral domain of charactesistic p, so all but the first and last terms in the sum must be zero. Therefore

$(a+b)^p = a^p+b^p$

Now suppose that the result hold for all k,

where $1 \le k \le n$, i.e, $(a+b)^{p^k} = a^{p^k}+b^{p^k}$.

By the induction hypothesis

$$\begin{aligned}(a+b)^{p^{k+1}} &= (a+b)^{p^k \cdot p}\\ &= \{(a+b)^p\}^{p^k}\\ &= (a^p+b^p)^{p^k}\\ &= (a^p)^{p^k}+ (b^p)^{p^k}\\ &= a^{p^{k+1}}+ b^{p^{k+1}}\end{aligned}$$

Therefore the result is true for n = k+1. Thus by the principle of mathematical induction, the result is true for any positive integer n, i.e.,

$(a+b)^{p^n} = a^{p^n}+b^{p^n}$ for all positive integer n.

Definition: Let F be a field. A polynomial $f(x) \in F[x]$ of degree n is separable if it has n distinct roots in the splitting field of f(x); i.e., f(x) is separable when it factors into distinct linear factors over the splitting field of f. An extension E of F is a separable extension of F if every element of E is the root of a separable polynomial in F[x].

Example : The polynomial x^2-2 is separable over Q since it factors as $\left(x-\sqrt{2}\right)\left(x+\sqrt{2}\right)$. In fact, $Q\left(\sqrt{2}\right)$ is a separable extension of Q.

Lemma 11.8.3. Let F be a field and $f(x) \in F[x]$. Then f(x) is separable if and only if f(x) and its derivative f'(x) are relatively prime.

Proof : Let f(x) be separable. Then f(x) factors over some extension field of F as

$f(x) = (x-\alpha_2)(x-\alpha_3)\ldots(x-\alpha_n)$ where ($\alpha_i \neq \alpha_j$ for $i \neq j$

Taking the derivative of f(x). We get

$f'(x) = (x-\alpha_2)(x-\alpha_3)\ldots(x-\alpha_n) + (x-\alpha_1)(x-\alpha_3)\ldots(x-\alpha_n)$

$+(x-\alpha_1)(x-\alpha_2)(x-\alpha_4)\ldots(x-\alpha_n) + \ldots + (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_{n-1})$

Hence f(x) and $f'(x)$ have no common factors, i.e. f(x) and $f'(x)$ are relatively prime.

To prove the converse, we will show the contrapositive of the statement is true, i.e. we show the statement "if f(x) is not separable, then f(x) and $f'(x)$ are not relatively prime" is true.

Let f(x) is not separable and

$f(x) = (x-\alpha)^k g(x)$, where $k > 1$.

Then $f'(x) = k(x-\alpha)^{k-1} g(x) + (x-\alpha)^k g'(x)$

Therefore f(x) and $f'(x)$ have a common factor, i.e. f(x) and $f'(x)$ are not relatively prime.

Thus the contrapositive statement is true and henve if f(x) and $f'(x)$ are relatively prime, then f(x) is separable.

Theorem 11.8.4. for every prime p and every positive integer n, there exists a finite field F with p^n elements. Furthermore, any field of order p^n is isomorphic to the splitting field of $x^{p^n}-x$ over Z_p.

Proof : Let $f(x) = x^{p^n}-x$ and let F be the splitting field of f(x). Then f(x) has p^n distinct zeros in F, since $f'(x) = p^n x^{p^n-1}-1 = -1$ is relatively prime to f(x).

We claim that the roots of f(x) form a subfield of F. Certainly 0 and 1 are zeros of f(x). If α and β are zeros of f(x), then $\alpha+\beta$ and $\alpha\beta$ are also zeros of f(x), since

$\alpha^{p^n} + \beta^{p^n} = (\alpha+\beta)^{p^n}$ and $\alpha^{p^n}\beta^{p^n} = (\alpha\beta)^{p^n}$.

We also need to show that the additive inverse and multiplicative inverse of each zero of f(x) are zeros of f(x). For any zero α of f(x), we know that $-\alpha$ is also a zero of f(x), since

$f(-\alpha) = (-\alpha)^{p^n} - (-\alpha)$

$= -\alpha^{p^n} + \alpha$, if p is odd

$= -\left(\alpha^{p^n} - \alpha\right)$

= 0

If p = 2, then $f(-\alpha) = (-\alpha)^{2^n} - (-\alpha) = \alpha + \alpha = 2\alpha = 0$

If $\alpha \neq 0$ then $\left(\alpha^{-1}\right)^{p^n} = \left(\alpha^{p^n}\right)^{-1}$

$= \alpha^{-1}$

Since the zeros of f(x) form a subfield of F and f(x) splits in this subfield, so the subfield must be all of F.

Let E be any other field of order p^n. To show that E is isomorphic to F, we must show that every element in E is a zero of f(x). Certainly 0 is a zero of f(x). Let α be any nonzero element of E. The order of the multiplicative group of nonzero elements of E is p^n–1; hence

$$\alpha^{p^n-1} = 1$$

$$\Rightarrow \alpha^{p^n} = \alpha$$

$$\Rightarrow \alpha^{p^n} - \alpha = 0$$

$$\Rightarrow f(\alpha) = 0$$

Since E contains p^n elements, E must be a splitting field of f(x). Since for each $p(x) \in F[x]$, there exists a splitting field K of p(x) that is unique upto isomorphism, therefore $E \cong F$.

The unique finite field with p^n elements is called the Galois field of order p^n. We will denote this field by GF (p^n).

11.9 PROPERTIES OF FINITE FIELDS

Theorem 11.9.1 As a group under addition, GF(p^n) is isomorphic to $Z_p \oplus Z_p \oplus .... \oplus Z_p$

As a group under multiplication, the set of non zero elements of GF(p^n) is isomorphic to Z_{p^n-1} (and is, therefore, cyclic).

Proof : Since GF(p^n) has characteristic p, every nonzero element of GF(p^n) has additive order p. Then by the fundamental theorem of finite abelian groups, GF(p^n) under addition is isomorphic to a direct product of n copies of Z_p.

Since the multiplicative group GF(p^n) of nonzero elements of GF(p^n) is cyclic, so by fundamental theorem of finite abelian groups, GF(p^n) is isomorphic to a direct product of the form $Z_{n_1} \oplus Z_{n_2} \oplus .... \oplus Z_{n_m}$. If the orders of this components are pairwise relatively prime, then GF(p) is cyclic. If not, we assume there is an integer d >1 that divides the orders of two of the

components. From the fundamental theorem of cyclic group, we know thateach of these components has a subgroup of order d. This means that GF(p) has two distinct subgroups of order d, call them H and K. But then every element of H and K is a zero of x^d–1, which contradicts the fact that a polynomial of degree d over a field can have at most d zeros. Hence the order of these components are pairwise relatively prime and which implies $GF(p^n)$ is cyclic. Thus the p^n–1 nonzero elements of $GF(p^n)$ form a cyclic group under multiplication and so is isomorphic to Z_{p^n-1}.

Corollarly 11.9.2. $GF(p^n)$ forms a rector space of dimension n over GF(p), i.e., $[GF(p^n) : GF(p)] = n$.

Proof : Since we know that $GF(p^n)$ as an additive group is isomorphic to $Z_p \oplus Z_p \oplus .... \oplus Z_p$ (n times), so we just need to find a basis for this over $GF(p) \cong Z_p$. Since $Z_p \oplus Z_p \oplus .... \oplus Z_p$ is a vector space over Z_p with {(1, 0, 0, . . .0), (0, 1, 0, . . ., 0) . . ., (0, 0, 0, . . ., 1)} as a basis, therefore

$[GF(p^n) : GF(p)] = n$

Corollary 11.9.3. Let a be a generator of the group of nonzero elements of $GF(p^n)$ under multiplication. Then a is algebraic over GF(p) of degree n.i.e. deg(a, GF(p)) = n.

Proof : SInce a generates all nonzero elements of $GF(p^n)$ (under multiplication) and $0 \in GF(p)$, therefore $GF(p)(a) = GF(p^n)$. and

$[gf(p)(a) : GF(p)]$

$= [GF(p^n) : GF(p)]$

$= n$

Also since a generates all nonzero element of $GF(p^n)$ so a generates 1 and $a^m = 1$ for some $m \in N$. Therefore a is algebraic over GF(p) since a is a zero of $p(x) = x^m - 1 \in GF(p)[x]$. If deg(a, GF(p)) = l, then $GF(p)(a) = GF(p^n)$ is an l-dimensional vector space over GF(p) with basis $\{1, a, a^2, . . ., a^{l-1}\}$. But all bases of $GF(p^n)$ have the same size, so

deg(a, GF(p)) = l = n

Corollary 11.9.4. If F is any finite field, then for every posible integer n, there is an irreducible pdynomial in F[x] of degree n.

Notes :

(i) Corollary 11.9.4. implies that no finite field is algebraically closed,

(ii) For any prime p and $n \in N$, if E and E' are fields of order p, then $E \cong E$.

(iii) Fundamental Theorem of Finite Fields : A finite field of order m exists if and only if $m = p^n$ for some prime p and some $n \in IN$. In addition, all fields of order p^n are isomorphic.

(iv) We have a clear idea of the structure of finite field GF(p) since $GF(p) \cong Z_p$.

Example : We construct GF(16). Of course GF (16) is of characteristic 2. So GF (16) has Z_2 as a subfield. So we will construct GF (16) as an algebraic extension field of Z_2. F[x]/<irr(α,F)> is an extension field of field F where $\alpha \notin F$ is algebraic over F. So we want to find an irreducible polynomial $p(x) \in Z_2[x]$ of degree 4. Then the elements of $Z_2[x]$/<p(x)> will be polynomials of degree 3 or less and there will be 2^4=16 such polynomials.

Let $p(x) = x^4+x+1 \in Z_2[x]$. Since neither 0 nor 1 is a zero of p(x), therefore it has no linear factors. The only possible quadratic factors are x^2+x+1 and x^2+1 and neither of these is a factor. So p(x) is irreducible. We take the elements of $Z_2[x]$ / <p(x)> to be cosets of <p(x)> in which addition is done as usual in $Z_2[x]$ but multiplication is done "modulo p(x)". Since the product of polynomials will be reduced modulo p(x), therefore all elements of $Z_2[x]$ /<p(x)> will be represented by polynomials of degree 3 or less and hence there will be 2^4 = 16 of them.

So, GF (16) = $\{ax^3+bx^2+cx+d : a, b, c, d \in Z_2\}$

We denote these as :

$g_0 = 0x^3+0x^2+0x+0 = 0$ $g_8=1x^3+0x^2+0x+0 = x^3$

$g_1 = 0x^3+0x^2+0x+1 = 1$ $g_9=1x^3+0x^2+0x+1 = x^3+1$

$g_2 = 0x^3+0x^2+1x+0 = x$ $g_{10}=1x^3+0x^2+1x+0 = x^3+x$

$g_3 = 0x^3+0x^2+1x+1 = x+1$ $g_{11}=1.x^3+1x^2+0.x+0 = x^3+x$

$g_4 = 0x^3+1x^2+0x+0 = x^2$ $g_{12}=1.x^3+1x^2+0.x+1 = x^3+x^2+1$

$g_5 = 0.x^3+1x^2+0x+1 = x^2+1$ $g_{13}=1.x^3+1.x^2+1.x+0 = x^3+x^2+x$

$g_6 = 0x^3+1x^2+1x+0 = x^2+x$ $g_{14}=1x^3+0.x^2+1x+1 = x^3+x^2+1$

$g_7 = 0x^3+1x^2+1x+1 = x^2+x+1$ $g_{15}=1x^3+1x^2+1x+1 = x^3+x^2+x+1$

Theorem 11.9.5. Every subfield of the field GF(p^n) has p^m elements, where m divides n. Conversely, if m|n for m > 0, then there exists a unique subfield of GF (p^n) is isomorphic to GF(p^m).

Example 1. Let F be the field of order 16. Then there are exactly three subfields of F, and their orders are 2, 4 and 16. Obviously, the subfield of order 2 is {0, 1} and the subfield of order 16 is F itself. To find the subfield of order 4, we merely observe that the three nonzero elements of this subfield must be the cyclic subgroup of F = $< x >$ of order 3. So the subfield of order 4 is $\{0, 1, x^5, x^{10}\} = \{0, 1, x^2+x, x^2+x+1\}$ since the nonzero elements of GF (16) form a cyclic group of order 15 and $g_2 = x$ is its generator as

$g_2 = x$

$g_2^2 = x^2 = g_4$

$g_2^3 = x^3 = g_8$

$g_2^4 = x^4 \equiv x+1 = g_3$

$g_2^5 = x(x+1) = x^2+x = g_6$

$g_2^6 = x(x^2+x) = x^3+x^2 = g_{12}$

$g_2^7 = x(x^3+x^2) = x^4+x^3 \equiv x^3+x+1 = g_{11}$

$g_2^8 = x(x^3+x+1) = x^4+x^2+x \equiv x^2+1 = g_5$

$g_2^9 = x(x^2+1) = x^3+x = g_{10}$

$g_2^{10} = x(x^3+x) = x^4+x^2 \equiv x^2+x+1 = g_7$

$g_2^{11} = x(x^2+x+1) = x^3+x^2+x = g_{14}$

$g_2^{12} = x(x^3+x^2+x) = x^4+x^3+x^2 = x^3+x^2+x+1 = g_{15}$

$g_2^{13} = x(x^3+x+x+1) = x^4+x^3+x^2+x \equiv x^3+x^2+1 = g_{13}$

$g_2^{14} = x(x^3+x^2+1) = x^4+x^3+x = x^3+1 = g_9$

$g_2^{15} = x(x^3+1) = x^4+1 \equiv 1 = g_1$

Example : The lattice of subfields of GF (p^{24}) is given in figure 11.1

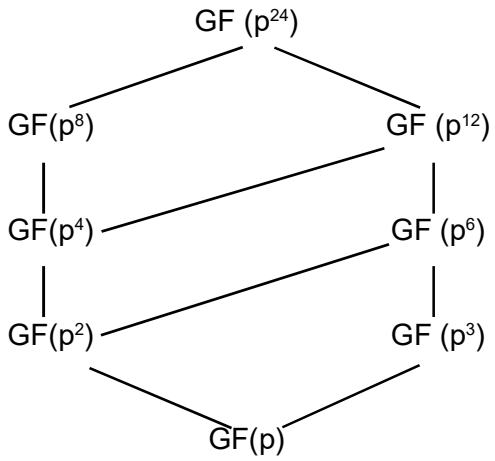


Figure 11.1



CHECK YOUR PROGRESS

Q 11: Write the subfield lattice of $GF(2^{24})$.

Q 12: If m|n, show that $[GF(p^n) : GF(p^m)] = \frac{n}{m}$

Q 13: Calculate each of the followings :

(i) $[GF(3^6) : GF(3^3)]$

(ii) $[GF(64) : GF(8)]$

(iii) $[GF(p^{12}) : GF(p^2)]$ where p is a prime



11.10 LET US SUM UP

- Let R be a commutative ring. The set $R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 | a_i \in R$ and n is a nonegative integer$\}$ form a ring under addition and multiplication of polynomials. This ring is called polynomial ring over R in the indeterminate x.
- Let R[x] be the polynomial ring over a ring R. Then
  (i) R is commutative if and only if R[x] has commutative.
  (ii) R has unity if and only if R[x] has unity.
  (iii) R is integral domain if and only if R[x] is an integral domain.
  (iv) If R is a field, then R[x] may not be a field.
- Let R be a commutative ring with unity and g(x), a nonzero polynomial in R[x] of degree n with leading coefficient b_n unit in R. Then for any $f(x) \in R[x]$ there exist unique polynomial q(x), r(x) in R[x] such that
  $f(x) = g(x)\, q(x) + r(x)$
  Where r(x) = 0 or deg r(x) < deg g(x).
- A polynomial $f(x) \in D$, D is an integral domain, is said to be an irreducible polynomial over D if it cannot be expressed as product of two polynomials of positive degree, i.e., if whenever f(x) = g(x) h(x), then deg g(x) = 0 or deg h(x) = 0.
  A polynomial $f(x) \in D$ is called reducible if it is not irreducible over D.
- If $f(x) \in Z[x]$ is reducible over Q, then it is reducible over Z.

- Eisenstein's Criterion for irreducibility : Let $f(x) = a_n x^x + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in Z[x]$.
  If there is a prime p such that $p \not| a_n$, $p|a_{n-1}, \ldots p|a_0$ and $p^2|a_0$, then f(x) is irreducible over Q.
- For every prime p and every positive integer n, there exists a finite field F with p^n elements. Further more, any field of order p^n is isomorphic to the splitting field of $x^{p^n}-x$ over Z_p.



11.11 FURTHER READINGS

1) Gallian, Joseph A. : Contemporary Abstract algebra (8th Ed.), Cengage Learning India Pvt. Ltd, Delhi 110092.
2) Fraleigh John B. : A first course in Abstract Algebra (2003), Pearson Educarion (Singapure) Pvt. Ltd, India Branch, Delhi 110092.
3) Khanna, V. K. and Bhambri, S. K. : A course in Abstract Algebra (2002), Vikas Publishing House Pvt. Ltd, New Delhi 110014.
4) Thomas, Judson W. : Abstract Algebra : Theory and Applications (2020), Libra Texts, https://math.libretexts.org/@go/page/81019.



11.12 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: We have $f(x) = 1 + 2x + 3x^2 \in Z_6[x]$

and $g(x) = 2 + 4x + 2x^2 \in Z_6[x]$

$\therefore$ $f(x) + g(x) = (1+2) + (2+4)x + (3+2)x^2$

$= 3+0x+5x^2$

$= 3 + 5x^2$

and deg $(f(x) + g(x)) = 2$

Here $a_0 = 1, a_1 = 2, a_2 = 3, a_3 = 0, a_4 = 0$

$b_0 = 2, b_1 = 4, b_2 = 2, b_3 = 0, b_4 = 0$

$f(x)\ g(x) = c_1+c_1x+c_2x^2+c_3x^3+c_4x^4$

Where $c_0 = a_0b_0 = 1.2 = 2$

$c_1 = a_0b_1 + a_1b_0 = 1.4+2.2 = 8 = 2$

$c_2 = a_0b_2 + a_1b_1 + a_2b_0 = 1.2+2.4+3.2 = 16 = 4$

$c_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 = 1.0+2.2+3.4+3.0 = 16 = 4$

$c_4 = a_0b_4 + a_1b_3 + a_2b_2 + a_3b_1 + a_4b_0$

$= 1.0+2.0+3.2+0.4+0.2$

$= 6$

$= 0$

$\therefore$ $f(x)g(x) = 2+2x+4x^2+4x^3+0.x^4$

$= 2+2x+4x^2+4x^3$

and deg $(f(x).g(x)) = 3$

Ans to Q No 2: We have $f(x) = 2+3x+4x^2+2x^3 \in Z_5[x]$

$g(x) = 4+2x+2x^4 \in Z_5[x]$

Here $a_0 = 2, a_1 = 3, a_2 = 4, a_3 = 2, a_4 = 0, a_5 = 0, a_6 = 0, a_7 = 0$

$b_0 = 4, b_1 = 2, b_2 = 0, b_3 = 0, b_4 = 3, b_5 = 0, b_6 = 0, b_7 = 0$

$\therefore$ $f(x)+g(x) = (2+4)+(3+2)x+(4+0)x^2+(2+0)x^3+(0+3)x^4$

$= 6+5x+4x^2+2x^3+3x^4$

$= 1+0.x+4x^2+2x^3+3x^4$

$= 1+4x^2+2x^3+3x^4$

and deg $(f(x)+g(x)) = 4$

$f(x).g(x) = c_0+c_1x+c_2x^2+c_3x^3+c_4x^4+c_5x^5+c_6x^6+c_7x^7$

Where $c_0 = a_0b_0 = 2.4 = 8 = 3$

$c_1 = a_0b_1+a_1b_0 = 2.2+3.4 = 16 = 1$

$c_2 = a_0b_2+a_1b_1+a_2b_0 = 2.0+3.2+4.4 = 22 = 2$

$c_3 = a_0b_3+a_1b_2+a_2b_1+a_3b_0 = 2.0+3.0+4.2+2.4 = 16 = 1$

$c_4 = a_0b_4+a_1b_3+a_2b_2+a_3b_1+a_4b_0$

$= 2.3 + 3.0 + 4.0 + 2.2 + 0.4$

$= 10$

$= 0$

$c_5 = a_0b_5+a_1b_4+a_2b_3+a_3b_2+a_4b_1+a_5b_0$

$= 2.0 + 3.3 + 4.0 + 2.0 + 0.2 + 0.4$

$= 9$

$= 4$

$c_6 = a_0b_6+a_1b_5+a_2b_4+a_3b_3+a_4b_2+a_5b_1+a_6b_0$

$= 2.0 + 3.0 + 4.3 + 2.0 + 0.2 + 0.2 + 0.4$

$= 12$

$= 2$

$c_7 = a_0b_7+a_1b_6+a_2b_5+a_3b_4+a_4b_3+a_5b_2+a_6b_1+a_7b_0$

$= 2.0 + 3.0 + 4.0 + 2.3 + 0.0 + 0.0 + 0.2 + 0.4$

$= 6$

$= 1$

$\therefore$ $f(x) \cdot g(x) = 3 + x + 2x^2 + x^3 + 0.x^4 + 4x^5 + 2x^6 + x^7$

and deg $(f(x) \cdot g(x)) = 7$

Ans to Q No 3: Given, R is a ring and

$R[x] = \{f(x) = a_0+a_1x+a_2x^2 + \ldots + a_mx^m : a_0, a_1, a_2, \ldots, a_m \in R$ and m ia a nonegative integer}. We have to prove R[x] is a ring under addition and multiplication of polynomial. We prove the followings :

(i) R[x] is an abelian group under addition of polynomials.

(ii) R[x] is a semi group under multiplication of polynomials.

(iii) Distributive laws are statisfied by the polynomials in R[x].

(I) Let $f(x), g(x) \in R[x]$, where

$f(x) = a_0+a_1x+a_2x^2 + \ldots + a_mx^m$, $a_i \in R \ \forall$ i = 0, 1, 2, 3, . . ., m

$g(x) = b_0+b_1x+b_2x^2 + \ldots + b_nx^n$, $b_i \in R \ \forall$ i = 0, 1, 2, 3, . . ., n

Then $f(x)+g(x) = c_0+c_1x+c_2x^2 + \ldots + c_tx^t$

Where $c_i = a_i + b_i \ \forall$ i and $t \leq \max \{m, n\}$

Since for each i, $c_i \in R$, therefore

$f(x) + g(x) \in R[x]$

Hence addition of polynomials is a binary operation in R[x]

Associativity of polynomials in R[x] follows from the associativity in R under addition.

The zero polynomial $0 = 0 + 0x + 0x^2 + \ldots \in R[x]$ is the additive identity.

The additive inverse of each polynomial $f(x) = a_0+a_1x+a_2x^2 + \ldots + a_mx^m \in R[x]$ is the polynomial $-f(x) = (-a_0) + (-a_1)x + (-a_2)x^2 + \ldots + (-a_m)x^m \in R[x]$.

The commutativity of polynomial addition in R[x] follows from the commutativity of addition in R.

Thus R[x] is an abelian group under addition polynomials.

(II) $f(x)\, g(x) = d_0+d_1x+d_2x^2+ \ldots + d_px^p$.

Where $d_k = \sum_{i+j=k} a_i d_j$ and $p \leq m+n$

Since $d_k \in R \; \forall \; k \in \{0, 1, 2, \ldots, p\}$, therefore $f(x) \,.\, g(x) \in R[x]$

Hence R[x] is closed under multiplication of polynomials.

Associativity of polynomial multiplication in R[x] follows from the associativity of multiplication in R.

Thus R[x] is a semi-group under multiplication of polynomials.

(III) The distributive laws in R[x] hold as distributive laws hold in R.

Hence R[x] is a ring.

Ans to Q No 4: Define a mapping $\phi : R[x] \to \frac{R}{A}[x]$ by

$\phi(f(x)) = \phi(a_0+a_1x+ \ldots + a_nx^n)$

$= (a_0+A) + (a_1+A)x + \ldots + (a_n+A)x^n$

Then ϕ is clearly well defined.

Let $f(x) = a_0+a_1x+a_2x^2 + \ldots + a_nx^n \in R[x]$

and $g(x) = b_0+b_1x+b_2x^2 + \ldots + a_mx^m \in R[x]$.

Then $f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x + (a_2+b_2)x^2 + \ldots + (a_t+b_t)x^t$

Where $t = \max \{n, m\}$

and $f(x)\, g(x) = c_0+c_1x+c_2x^2 + \ldots + c_lx^l$

Where $c_k = \sum_{i+j=k} a_i d_j$ and $0 \leq k \leq l$, $l \leq m+m$.

$\phi(f(x)+g(x)) = \phi((a_0+b_0) + (a_1+b_1) + (a_2+b_2)x^2 + \ldots)$

$= [(a_0+b_0)+A] + [(a_1+b_1) + A]\, x + [(a_2+b_2) + A]x^2 + \ldots$

$= [(a_0+A)+(b_0+A)] + [(a_1+A) + (b_1+A)]\, x + [(a_2+A)$

$+(b_2+A)]x^2+ \ldots$

$= [(a_0+A)+(a_1+A)x + (a_2+A)x^2 + \ldots] + [(b_0+A)\, (b_1+A)x$

$+(b_2+A)x^2+ \ldots]$

$= \phi[f(x)] + [g(x)]$

$\phi(f(x).g(x)) = \phi(c_0+c_1x + c_2x^2 + \ldots)$

$= (c_0+A)+ (c_1+A) + (c_2+A)x^2 + \ldots$

$= (a_0b_0+A)+(a_1b_0+a_0b_1+A)x + (a_2b_0+a_1b_1+a_0b_2+A)x^2+ \ldots$

$= (a_0+A)\, (b_0+A) + [(a_1+A)(b_0+A) + (a_0+A)(b_1+A)]x + [(a_2+A)$

$(b_0+A) + (a_1+A)\, (b_1+A)+(a_0+A)\, (b_2+A)]\, x^2 + \ldots$

$= (a_0+A)\, [(b_0+A) + (b_1+A)x + (b_2+A)x^2 + \ldots] + (a_1+A)x$

$[(b_0+A) + (b_1+A)x + (b_2+A)x^2 + \ldots] + (a_2+A)x^2\,[(b_0+A) + (b_1+A)x + (b_2+A)x^2 + \ldots] + \ldots\ldots$

$= [(a_0+A) + (a_1+A)x + (a_2+A)x^2 + \ldots]\,[(b_0+A) + (b_1+A)x + (b_2+A)x^2 + \ldots]$

$= \phi[f(x)]\,\phi[g(x)]$

$\therefore \phi$ is a ring homomorphism.

That ϕ is onto is evident from the definition, hence by fundamental theorem of ring homomorphism,

$$\frac{R[x]}{\ker\phi} \cong \frac{R}{A}[x]$$

Where $\ker\phi = \{a_0+a_1x+a_2x^2+\ldots+a_mx^m : \phi(a_0+a_1x+a_2x^2+\ldots+a_mx^m) = A\}$

$= \{a_0+a_1x+\ldots+a_mx^m : (a_0+A)+(a_1+A)x + \ldots + (a_m+A)x^m = (0+A)+(0+A)x + \ldots+ (0+A)x^m\}$

$= \{a_0+a_1x+\ldots+a_mx^m : a_0+A=A,\ a_1+A = A,\ \ldots,\ a_m+A = A\}$

$= \{a_0+a_1x+\ldots+a_mx^m : a_0 \in A,\ a_1 \in,\ \ldots,\ a_m \in A\}$

$= A[x]$

Hence $\dfrac{R[x]}{A[x]} \cong \dfrac{R}{A}[x]$

Ans to Q No 5: Define a map $\psi : R[x] \to R$ by

$\psi(a_0+a_1x+\ldots+a_nx^n) = a.$

Then ψ is clearly well defined. Also

$\psi[(a_0+a_1x+\ldots+a_nx^n) + (b_0+b_1x+\ldots+b_mx^m)]$

$= \psi[(a_0+b_0) + (a_1+b_1)x + \ldots]$

$= a_0+b_0$

$= \psi(a_0+a_1x+\ldots+a_nx^n) + \psi(b_0+b_1x+\ldots+b_mx^m)$

Similarly the result for product follows.

Thus ψ is a ring homomorphism which is clearly onto. By fundamental theorem of ring homonophism, we get

$$\frac{R[x]}{\ker\psi} \cong R$$

Let $f(x) = a_0+a_1x+\ldots+a_nx^n \in \ker\psi$. Then

$\psi(a_0+a_1x+\ldots+a_nx^n) = 0$

$\Rightarrow a_0 = 0$

$\therefore$ $f(x) = a_1x + a_2x^2 + \ldots + a_nx^n$

$= x(a_1x + a_2x^2 + \ldots + a_nx^{n-1})$

$= xh(x)$ (say), where $h(x) = a_1+a_2x + \ldots +a_nx^{n-1} \in R[x]$

$\therefore$ $f(x) \in \langle x \rangle$. Hence $\ker\psi = \langle x \rangle$.

Ans to Q No 6: Let R be a commutative ring with unity and $\langle x \rangle$ be a prime ideal of R[x]. We have to prove R is an integral domain.

Since R is a commutative with unity, therefore to prove R is an integral domain it is sufficient to prove that R is without zero disisor.

Let a a, $b \in R$ be such that ab = 0. Then the polynomials

$(0 + 1x + 0x^2 + \ldots) + (a + 0x + 0x^2 + \ldots)$ and

$(0 + 1x + 0x^2 + \ldots) + (b + 0x + 0x^2 + \ldots)$ belong to R[x].

$\Rightarrow x+a, x+b \in R[x]$

$\Rightarrow (x+a)(x+b) \in R[x]$

$\Rightarrow x^2+x(a+b) + ab \in R[x]$

Since ab = 0, $x^2+x(a+b) = x(x+a+b) \in \langle x \rangle$. Thus

$(x+a)(x+b) \in \langle x \rangle$

$\Rightarrow x+a \in \langle x \rangle$ or $x+b \in \langle x \rangle$ [$\because \langle x \rangle$ is prime ideal]

Now $(x+a) \in \langle x \rangle \Rightarrow x+a = xf(x)$ for some $f(x) \in R[x]$

$= x(a_0+a_1x + \ldots)$

Similary, if $x+b \in \langle x \rangle \Rightarrow b = 0$.

Hence R is an integral domain.

Ans to Q No 7: (i) Let $f(x) = 8x^3 - 6x - 1$

Since there is no prime which divides 1, we cannot apply the Eisenstein's criterion to f(x).

Consider $f(x+1) = 8(x+1)^3 - 6(x+1) - 1$

$= 8x^3 + 24x^2 + 18x + 1$

We have the same situation. Let us consider

$f(x-1) = 8(x-1)^3 - 6(x-1) - 1$

$= 8x^3 - 24x^3 + 18x - 3$

Take p = 3. Then $3|3$, $3|18$, $3|24$, $3 \nmid 8$ and $3^2 \nmid 3$.

Hence by Eisenstein's Criterion,

f(x–1) is irreducible over Q.

$\Rightarrow$ f(x) is irreducible over Q.

(ii) $(x) = x^4 + x^3 + x^2 + x + 1.$

$$= \frac{(x-1)(x^4+x^3+x^2+x^2+x+1)}{x-1}$$

$$= \frac{x^5-1}{x-1}$$

$$\therefore f(x+1) = \frac{(x+1)^5-1}{(x+1)-1}$$

$$= \frac{(x^5+5x^4+10x^3+10x^2+5x+1)-1}{x}$$

$$= x^4 + 5x^3 + 10x^2 + 10x + 5$$

Let us take p = 5. Then

$5|5$, $5|10$, $5|10$, $5|5|$, $5 \nmid 1$ and $5^2 \nmid 5$

Hence by Eisenstein's Criterion,

f(x+1) is irreducible over Q.

$\Rightarrow$ f(x) is irreducible over Q.

Ans to Q No 8: $f(x) = x^2+1$ is irreducible over R but reducible over C since $x^2+1 = (x+i)(x-i)$.

Ans to Q No 9: Let $f(x) = x^2+1$. Here $f(x) \in Z_{11}[x]$, Z_{11} is a field and deg f(x)= 2. So we apply reducibility test for degree.

$\therefore$ f(0) = 1, f(1) = 2, f(2) = 5, f(3) = 10,

f(4) = 6, f(5) = 4, f(6) = 4, f(7) = 6

f(8) = 10, f(9) = 5, f(10) = 2

There is no zero of x^2+1 in Z_{11}, $f(x) = x^2+1$ is irreducible over Z_{11}.

Let $g(x) = x^2+x+4$. Here $f(x) \in Z_{11}[x]$, Z_{11} is a field and deg f(x) = 2. So we apply reducibility test of degree 2.

f(0) = 4, f(1) = 6, f(2) = 10, f(3) = 5,

f(4) = 2, f(5) = 2, f(6) = 2, f(7) = 5

f(8) = 10, f(9) = 6, f(10) = 4

There is no zero of $g(x) = x^2+x+4$ in Z_{11}, so g(x) is irreducible over Z_{11}.

Ans to Q No 10: (i) Here $f(x) = 3x^5 + 15x^4 - 20x^3 + 10x + 20$

and $a_0 = 20$, $a_1 = 10$, $a_2 = 0$, $a_3 = 20$, $a_4 = 15$, $a_5 = 3$

Consider p = 5, Then

$p|a_0$, $p|a_1$, $p|a_2$, $p|a_3$, $p|a_4$, $p \nmid a_5$ and $p^2|a_0$

i.e. 5|20, 5|10, 5|0, 5|20, 5|15, $5 \nmid 3$ and $5^2 \nmid 20$

Hence by Eisenstein's Criterion, f(x) is irreducible over Q.

(i) $f(x) = 3x^3+6x^2+2x+6$

Here $a_0 = 6$, $a_1 = 2$, $a_2 = 6$, $a_3 = 3$

Consider p = 2. Then 2|6, 2|2, 2|6|, $2 \nmid 3$ and $2^2 \nmid 6$

Hence by Eisenstein's Criterion, f(x) is irreducible over Q.

(iii) Here $f(x) = x^3+3x+2$

Since there is no prime p which divide both 2 and 3, so we cannot apply the Eisenstein's Criterion to f(x).

Consider $f(x+1) = (x+1)^3+3(x+1)+2$

$= x^3+3x^2+6x+6$

Take p = 3. Then

3|6, 3|6|, 3|3|, $3 \nmid 1$ and $3^2 \nmid 6$

Hence by Eisenstein's Criterion, f(x) is irreducible over Q.

Ans to Q No 11: The subfield lattice of GF (2^{24}) is the following :

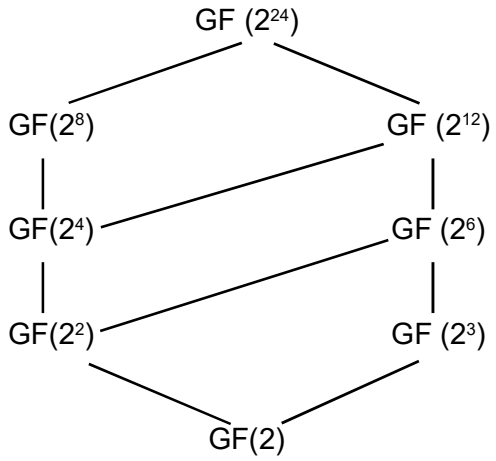


Figure 11.2

Ans to Q No 12: Let m|n. Then

$GF(p) \subseteq GF(p^m) \subseteq GF(p^n)$ and there fore

$[GF(p^n) : GF(p)] = [GF(p^n) : GF(p^m)] \,.\, [GF(p^m) : GF(p)]$

$\Rightarrow n = [GF(p^n) : GF(p^m)].m$

$\Rightarrow [GF(p^n) : GF(p^m)] = \frac{n}{m}$

Ans to Q No 13: (i) $[GF(3^6) : GF(3^3)] = \frac{6}{3} = 2$ [$\because$ 3|6]

(ii) $[GF(64) : GF(8)] = [GF(2^6) : GF(2^3)]$

$$= \frac{6}{3} \qquad [\because 3|6]$$

$$= 2$$

(iii) $[GF(p^{12}) : GF(p^2)] = \frac{12}{2}$ $[\because$ p is prime and $2|12]$

$$= 6$$



11.13 MODEL QUESTIONS

Q 1: Let $f(x) = 4x^3+2x^2+x+3$ and $g(x) = 3x^4+3x^3+3x^2+x+4$ where $f(x), g(x) \in Z_5[x]$. Compute $f(x)+g(x)$ and $f(x).g(x)$.

Q 2: Show that x^2+3x+2 has four zeros in Z_6.

Q 3: If R is a commutative ring, show that the characteristic of R[x] is the same as the characteristic of R.

Q 4: Let R be a commutative ring. Show that R[x] has a subring isomorphic to R.

Q 5: If $\phi : R \to S$ is a ring homomorphism and define $\bar{\phi}$:R[x] $\to$S[x] by $\bar{\phi}$ $(a_nx^n+a_{n-1}x^{n-1}+ \ldots + a_0) = \bar{\phi}(a_n)x^n + \bar{\phi}(a_{n-1})x^{n-1}+ \ldots + \phi(a_0)$, then show that $\bar{\phi}$ is a ring homomorphism.

Q 6: Let $f(x) = 5x^4+3x^3+1$ and $g(x) = 3x^2+2x+1$ in $Z_7[x]$. Determine the quotient and remainder upon dividing f(x) by g(x).

Q 7: Prove that the ideal $\langle x \rangle$ in Q[x] is maximal.

Q 8: Show that the following polynomials are irreducible over Q.

(i) $x^4 - 4x + 2$

(ii) $x^3 - 9x + 15$

(iii) $7x^4 - 2x^3 + 6x^2 - 10x + 18$

Q 9: Prove that x^2+1 and x^2+x+4 are irreducible over Z_{11}. Prove further that

$$\frac{Z_{11}[x]}{\langle x^2+1 \rangle} \cong \frac{Z_{11}[x]}{\langle x^2+x+4 \rangle}$$

each having 121 elements.

Q 10: Let F be a field and a be a nonzero element of F.

(a) If a(x) is irreducible over F, prove that f(x) is irreducible over F.

(b) If f(ax) is irreducible over F, prove that f(x) is irreducible over F.

(c) If f(x+a) is irreducible over F, prove that f(x) is irreducible over F.

Q 11: Draw the lattice of subfields of GH (64).

Q 12: Show that the Frobenius mapping ϕ: $GF(p^{n)} \rightarrow GF(p^n)$ given by $\phi(a) = a^p$, is a ring automorphism of order n.

Q 13: Let α be a zero of x^3+x^2+1 over Z_2. Construct a finite field of order 8. Show that x^3+x^2+1 splits in $Z_2(\alpha)$.

Q 14: Construct a finite field of order 27.

*** ***** ***